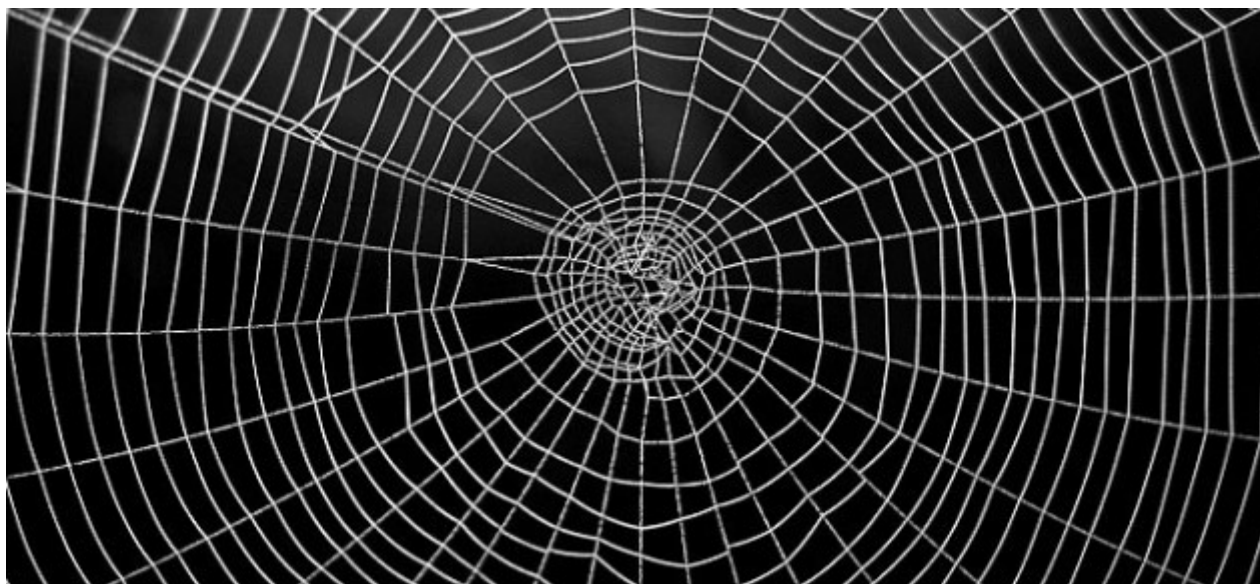


AUTODEFENSA DIGITAL



Guía práctica de comunicaciones protegidas para organizaciones sociales

Volumen 1.0 – ChatSecure



Grupo de
Autodefensa Digital



Índice

INTRODUCCIÓN.....	3
¿Qué es Construcción Tecnológica Popular?.....	3
¿Qué es el Grupo de Autodefensa Digital?.....	3
¿Por qué hacemos este manual?.....	4
¿Qué es un servidor?.....	5
¿Que ocurre cuando chateamos?.....	6
¿Quién es quién?.....	6
¿Qué es la criptografía?.....	8
¿Cómo hacemos una cuenta para tener conversaciones seguras con nuestrxs compañerxs?.....	9
INSTALACIÓN DE ChatSecure Y CREACIÓN DE UNA CUENTA EN EL SERVIDOR dukgo.com.....	11
¿Cómo instalamos ChatSecure en nuestro celular?.....	11
¿Cómo crear una cuenta en el servidor duckgo.com desde la aplicación para chatear ChatSecure?..	14
¿Cómo agregamos a un/a compañerx para conversar?.....	18
Encriptado de las comunicaciones.....	21
Activar el cifrado.....	23
Cómo autenticar.....	24
Terminar una conversación.....	29
CIERRE.....	29

INTRODUCCIÓN

¿Qué es Construcción Tecnológica Popular?

Construcción Tecnológica Popular (CTP) es una organización política enfocada en lo técnico. Quienes la conformamos partimos de la comprensión de que vivimos en una sociedad conflictiva, con jerarquías impuestas, como lo son el capitalismo, el patriarcado y el imperialismo.

La tecnología no es ajena a este conjunto de dominaciones, sino que cumple un rol activo en el sostenimiento de estas jerarquías. Nosotrxs tenemos la convicción de que También cumple y cumplirá un papel relevante para la resistencia y la creación de un mundo nuevo. Nos proponemos entonces disputar y colectivizar la tecnología que, en tanto construcción social, debe ser de todxs.

¿Qué es el Grupo de Autodefensa Digital?

El Grupo de Autodefensa Digital es un espacio impulsado por CTP en el que nos encontramos para generar estrategias de autodefensa digital, pensado especialmente para todxs aquellxs que se organizan colectivamente para cambiar la realidad. Nos proponemos explorar colectivamente diversas herramientas informáticas de seguridad y privacidad, los conocimientos que las sustentan y sus posibilidades de adaptación a distintas necesidades. Analizamos las estrategias de los grupos de poder en entornos digitales, para comprender su operatoria y los modelos de amenazas a los que nos encontramos expuestxs.

¿Por qué hacemos este manual?

Ésta pretende ser una pequeña guía de herramientas y recomendaciones que son sólo un primer paso para reducir la vulnerabilidad en las comunicaciones digitales de las organizaciones sociales en la coyuntura actual de Argentina.

Debemos tener siempre presente, como principio básico, que estas herramientas no son 100% efectivas y no ofrecen garantías de que nadie pueda espiarnos, pero sí de que le pondrán las cosas difíciles a quien quiera hacerlo.

Aunque la internet se ha vuelto la herramienta más completa de vigilancia a la sociedad civil, los métodos tradicionales siguen siendo igual de efectivos para el Estado y sus aparatos represivos, como es el caso de la infiltración de agentes en las organizaciones (podríamos citar el caso de la Agencia Rodolfo Walsh). Por esa razón creemos que nuestras organizaciones tienen que tener como pilar los métodos tradicionales de seguridad. Las nuevas tecnologías son el siguiente eslabón que tenemos que considerar.

Debemos tener en cuenta que los métodos de espionaje se han perfeccionado, la maquinaria de vigilancia no descansa y su funcionamiento eficiente es, por definición, no restrictivo sino silencioso, no reactivo sino retroactivo, no solo individual y dirigido, sino también masivo.

Debido a la vorágine de la innovación tecnológica, debemos advertir que este manual y las herramientas que presentamos son algo provisorio. Sirven, sí, pero solo por ahora, no sabemos si mañana, ni mucho menos si dentro de unos años.

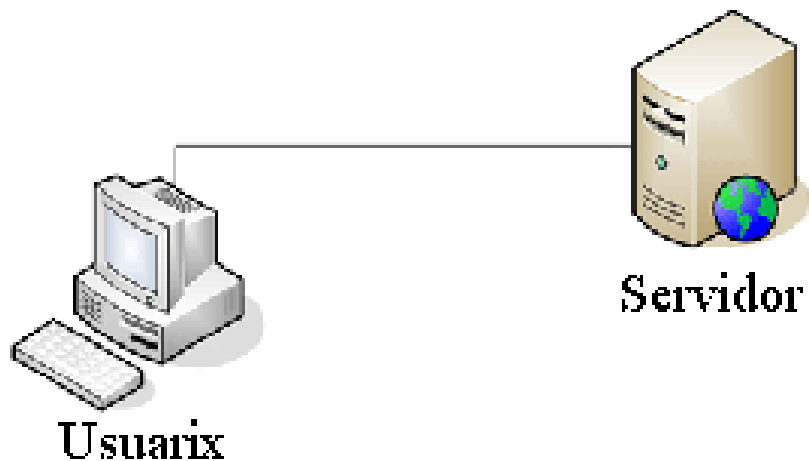
Expresamos nuestra firme convicción de que la seguridad y la privacidad de nuestros datos y comunicaciones son una construcción colectiva. Más allá de las herramientas que utilicemos, lo fundamental para construir una comunicación segura es afianzar las prácticas colectivas de seguridad (lo que decimos, la forma y el momento en que lo decimos) siendo indispensable la participación activa y consciente de cada unx de lxs compañerxs.

¿Qué es un servidor?

Un servidor es una computadora que tiene dueño y que está siempre encendida dentro de algún centro de datos, y que guarda y entrega información según se le pida.

Cuando entramos a una página de internet cualquiera (digamos el portal del diario La Voz del Interior), lo que nuestra computadora hace es enviar un pedido al **servidor** donde está guardada la información (fotos, textos, publicidades, etc.) para que nos la mande y nuestro **navegador** (Mozilla, Chrome, Explorer, etc.) nos la muestre.

Es decir, una computadora (la nuestra) envía un pedido a otra computadora (el servidor) para que le mande cierta información, esa información llega a la primer computadora y se muestra al usuario o la usuaria.



¿Que ocurre cuando chateamos?

Cuando mandamos un mensaje mediante Facebook (el ejemplo se aplicaría a Messenger, Hotmail, Twitter, etc.) lo que estamos haciendo es enviar una serie de datos desde una computadora a otra. Sin embargo, esa información no va a ir directamente desde nuestra computadora a la de nuestra compañera, primero pasará por el servidor de Facebook.

Nuestra computadora enviará el mensaje al servidor de Facebook diciéndole quiénes somos, dónde estamos y a quién le queremos enviar el mensaje. El servidor recibirá toda esa información (o “metadatos”) además del contenido del mensaje y recién ahí la enviará a la persona con la que nos queremos comunicar. Todo esto -metadatos y contenido de la comunicación- quedará registrado en el servidor de Facebook (o de cualquier otra empresa que utilicemos para comunicarnos).

Esto quiere decir que **cualquier conversación que tengamos por Facebook quedará guardada en los servidores de Facebook**. Esa conversación puede ser sobre amor, sobre una película que vimos, sobre organizar una fiesta, o puede ser (y esto es un problema) una conversación para organizar un taller de formación de nuestra organización, para distribuirnos las tareas para una movilización o para acordar una toma de tierras o cualquier otra acción colectiva.

Es decir, cuando usamos alguna plataforma virtual para comunicarnos y para organizarnos, no simplemente estamos haciendo eso, sino que además estamos haciendo pasar toda esa información por las computadoras de una empresa que la procesará, administrará y guardará.

¿Quién es quién?

Google, Facebook, Microsoft, Yahoo!, Twitter, etc., son empresas y, si bien todos los días nos vinculamos a ellas mediante sus servicios supuestamente **GRATUITOS**, responden a intereses capitalistas y tienen vínculos muy estrechos

con los estados y sus aparatos represivos.

¿Qué nos garantiza que una empresa privada no le vaya a dar registros de nuestras conversaciones a la policía que reprime o la justicia que criminaliza? **NADA**. De hecho ha pasado, y pasa todo el tiempo. Porque quien nos reprime, el estado -con sus fuerzas de seguridad y servicios de inteligencia- tiene vínculos e intereses en común con las empresas.

¿Cómo podemos hacer entonces para organizarnos y comunicarnos sin que todo lo que decimos llegue con copia a empresas y, por ende, posiblemente al estado?

Tenemos que pensar la solución en dos partes:

- 1) Tratar de que nuestros mensajes no pasen por los equipos (servidores) de empresas privadas.
- 2) Tratar de que si los mensajes que enviamos son interceptados no puedan ser comprendidos (“cifrar” o “encriptar” los mensajes).

Para que nuestras comunicaciones no pasen por los equipos de una empresa privada, vamos a tratar de elegir a otros proveedores de servicios de internet, que estén comprometidos con una ética de la privacidad y de la protección de los datos personales y colectivos.

En este caso recomendamos **DuckDuckGo**, que es un proveedor de servicios respetuoso de la intimidad y la privacidad de sus usuarios, que tiene un buscador web (como Google), pero que no te rastrea y no guarda la información de las búsquedas. El servicio que nos interesa para trabajar es el que nos ofrece de mensajería instantánea: **dukgo.com**¹.

¹ Vale aclarar que existen muchos proyectos de comunicación segura y respetuosa de la privacidad, que



DuckDuckGo

Para proteger el contenido de nuestras comunicaciones pensamos en dos elementos fundamentales: la criptografía y programas *libres*.

¿Que queremos decir cuando decimos programas libres?

Estamos pensando en programas que estén respaldados por una comunidad de desarrolladorxs y usuarixs que colaboran en su desarrollo y en los que toda la información de su funcionamiento está disponible para reproducirlos y, con los conocimientos suficientes, poder comprenderlos y modificarlos. Ejemplos conocidos de esto son los sistemas operativos GNU/Linux como Ubuntu y el navegador de internet Mozilla Firefox. “Libres” significa que no solo son gratuitos, sino también comunitarios, de “código abierto” y con términos legales de uso que son flexibles y solidarios.

¿Qué es la criptografía?

La criptografía es un conjunto de técnicas² desarrolladas para mantener el secreto de la información. Se aplica a correo, chat, redes sociales, llamadas, etc.; por ejemplo Riseup (riseup.net), un proyecto por y para militantes que se desarrolla en EEUU y cuyo uso está bastante difundido.

- 2 La criptografía se basa en operaciones matemáticas complejas que son procesadas por nuestras computadoras y que no son fáciles de “romper”. Los atacantes a menudo recurren a otras estrategias alternativas que desarrollaremos más adelante.

secreto en las comunicaciones de un extremo a otro, haciendo entendibles los mensajes en clave sólo para quienes están dirigidos. Así si un mensaje encriptado es interceptado, quien nos espíe solo obtendría un chorizo de letras y números sin sentido, es decir no podría interpretar el contenido. Es importante remarcar que existen técnicas y herramientas que pueden decifrar un mensaje encriptado, pero llevarlo a cabo es lento y costoso.

¿Cómo podemos tener conversaciones menos inseguras con nuestrxs compañerxs?

En las próximas secciones contamos como instalar la aplicación para chatear que nosotrxs proponemos (ChatSecure), aunque también existen otras. ChatSecure funciona en celulares que tengan Android.

Lo primero que debemos entender es que **existen dos componentes:** 1) **El programa o aplicación para chatear** y 2) **el servidor** donde estará alojada nuestra cuenta personal.

Generalmente estas dos cosas se nos presenta todo como un paquete cerrado (a nuestra cuenta de Facebook accedemos mediante la aplicación para chatear que nos impone Facebook, a nuestra cuenta de WhatsApp accedemos mediante la aplicación de WhatsApp que instalamos en nuestro celular, etc.), sin embargo, y sobretodo al trabajar con herramientas libres y seguras, la aplicación para chatear y nuestra cuenta alojada en un servidor son dos elementos separados y muy diferentes.

Desde un celular con sistema operativo Android, recomendamos usar **ChatSecure** como programa de mensajería, ya que es muy amigable, fácil de instalar y de configurar.



ChatSecure que es una aplicación de mensajería gratuita y de código abierto para telefonía celular que cuenta con cifrado OTR sobre el protocolo³ de chat XMPP (ya vamos a ver mejor que es esto).

Con ella podemos conectarnos a nuestras cuentas de chat ya existentes como las de Facebook, Gmail, RiseUp o crear cuentas nuevas en servidores públicos de XMPP, que es lo que nosotrxs vamos a hacer.

A diferencia de otros servicios de chat que nos mantienen cautivos con su propia aplicación, los servicios de chat XMPP cifrados con OTR son totalmente compatible con distintos programas de PC o aplicaciones móviles como ChatSecure, Pidgin, Jitsi, Conversations u otros.

Al utilizar esta aplicación vamos a poder comunicarnos con nuestrxs compañerxs de forma encriptada mediante cifrado **Off-the-Record (Fuera de Registro) (OTR)** que ofrece las siguientes funciones de seguridad y privacidad:

3 Lenguaje técnico en común que pueden usar dos computadoras para comunicarse entre sí.

Autenticación: Busca garantizar que el/la compañerx con quien nos comunicamos sea quien creemos que es.

Rechazo: Una vez finalizada la sesión de chat, no se puede identificar de dónde salieron o a dónde llegaron los mensajes.

Cifrado: Nadie puede interceptar nuestros mensajes en tránsito y leerlos (están en clave).

Perfecta seguridad adicional: En caso de que terceros obtengan nuestras propias claves privadas, ninguna de las conversaciones anteriores estará en peligro.

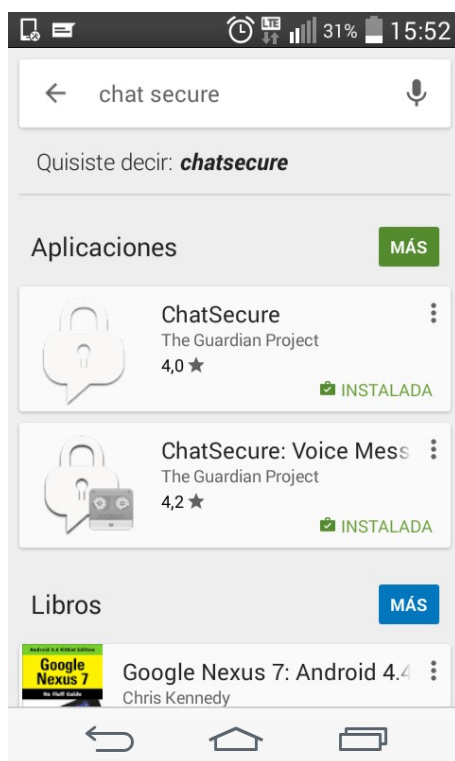
ChatSecure también permite iniciar chats en grupo y añadir nuevos contactos, lo cual se puede hacer desde el menú principal, pero es importante tener en cuenta que los grupos de chat no se pueden proteger, como los chats de uno-a-uno, debido a las limitaciones del protocolo OTR.

La aplicación es compatible con la mensajería multimedia, puede enviar fotos y archivos de forma segura si nuestrx compañerx también está utilizando cifrado de extremo a extremo, también llamado “de punto a punto” o “de par a par”.

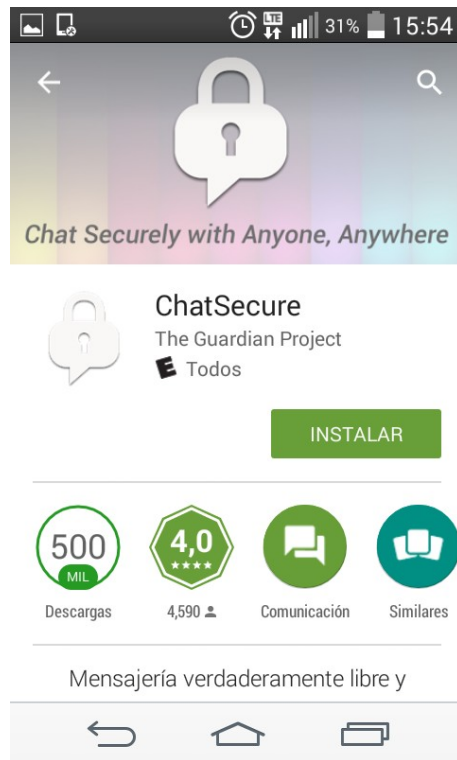
INSTALACIÓN DE ChatSecure Y CREACIÓN DE UNA CUENTA EN EL SERVIDOR dukgo.com

¿Cómo instalamos ChatSecure en nuestro celular?

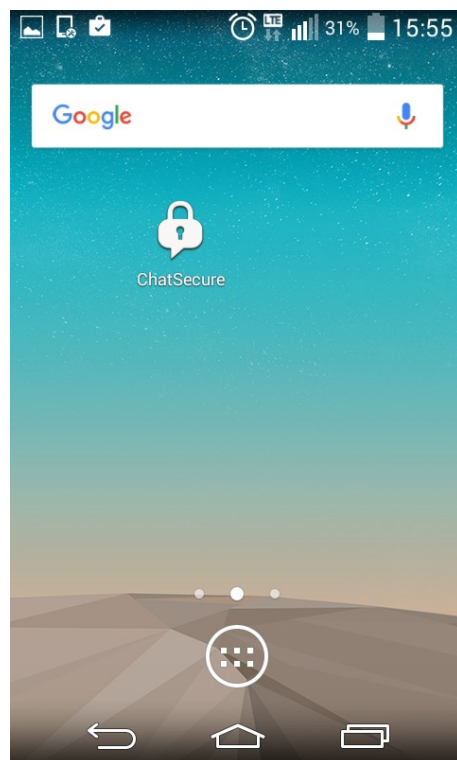
Desde el descargador de aplicaciones (Google Play por defecto en celulares con Android) debemos buscar ChatSecure.



Nos aparecerán distintas aplicaciones relacionadas a ChatSecure, y debemos elegir aquella que sólo dice “ChatSecure” y que tiene por desarrolladores a “The Guardian Project”. Luego de eso le damos a la opción “INSTALAR”.



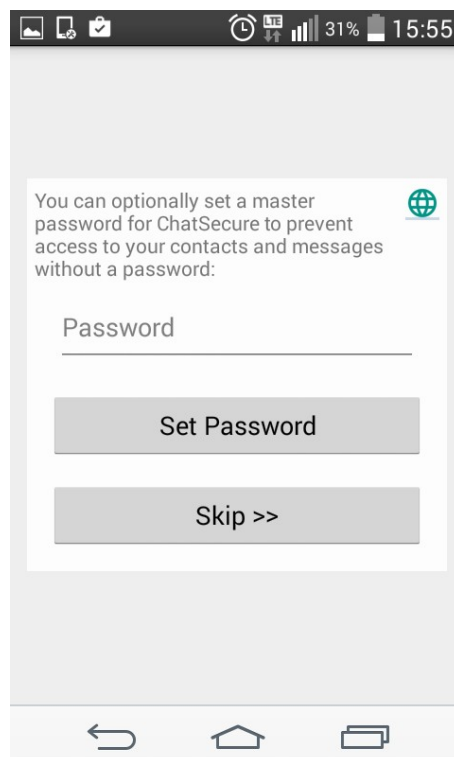
Una vez instalado nos aparecerá en nuestra pantalla del celular el icono de ChatSecure.



A continuación entramos a la aplicación ChatSecure y nos pedirá que elijamos una contraseña. En este punto resulta importante aclarar que estamos definiendo la clave para acceder a la aplicación para chatear ChatSecure, que es diferente a la clave de la cuenta que vamos a crear en el servidor duckgo.com. La clave que nos pide se usa para bloquear el acceso a la aplicación y a nuestras conversaciones. De esta forma sólo si conocemos dicha clave podremos leer las conversaciones en curso, continuarlas o iniciar otras nuevas sin tener que autenticarnos (ya vamos a ver de que se trata eso).

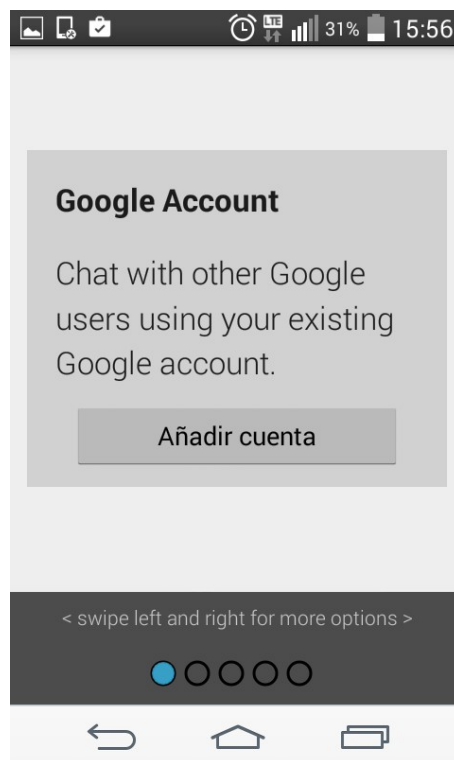
Retomando, la aplicación nos da la opción de poner una contraseña (“**Set Password**”) o de no ponerla (“**Skip>>**”). Nosotrxs recomendamos SIEMPRE usar contraseñas de aplicación, y que esas contraseñas no se repitan (no usar la misma en Facebook, Gmail y ChatSecure). A demás debe ser difícil de adivinar, con lo que NO debe hacer referencia a algo claramente cercano a nosotrxs, como nuestro DNI, fechas importantes, nombres de familiares o mascotas, etc.

Elegimos entonces la opción “**Set Password**”.

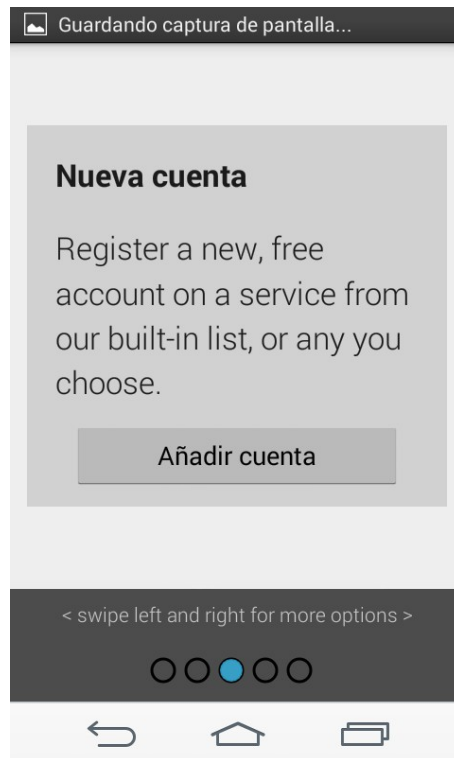


¿Cómo crear una cuenta en el servidor duckgo.com desde la aplicación para chatear ChatSecure?

Una vez elegida nuestra contraseña, nos aparecerá la siguiente pantalla en la que se nos ofrece conectar nuestro ChatSecure a una cuenta de Google, pero como lo que queremos es crear una cuenta en **dukgo.com**, pasaremos a la siguiente opción (deslizando la pantalla hacia la izquierda).



Avanzamos hasta llegar a la opción “**Nueva cuenta. Register a new, free account on a service from our built-in list, or any you choose**” y elegimos “**Añadir cuenta**”.



Nos aparecerán cuatro campos a llenar: nombre de usuario (“**new username**”), dominio del servidor que utilizaremos (“**Chat service domain**”), contraseña (“**contraseña**”) y confirmar contraseña (“**confirm password**”).

Añadir cuenta Jab... ELIMINAR CUENTA

new username

Chat service domain

contraseña

confirm password

Register Account

☒ Recordar

☐ Conectar a través de Tor (Requiere la aplicación Orbot)

Configuración avanzada de la cuenta

Lo que estamos por hacer es crear una cuenta en **dukgo.com**, que tendrá por nombre de usuario y contraseña los que ingresemos ahora.

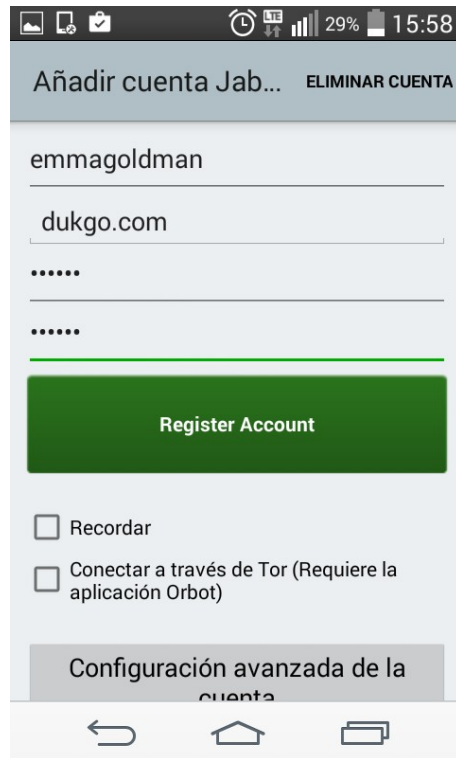
En el ejemplo, el nombre de usuario será *emmagoldman*. Cada uno debe ingresar el nombre que elija, preferentemente que no refleje nuestra identidad real.

En el dominio del servidor que utilizaremos (“*Chat service domain*”) ingresamos **dukgo.com**.

Ingresamos la contraseña que deseamos en “**contraseña**”, y la volvemos a ingresar en “**confirm password**”

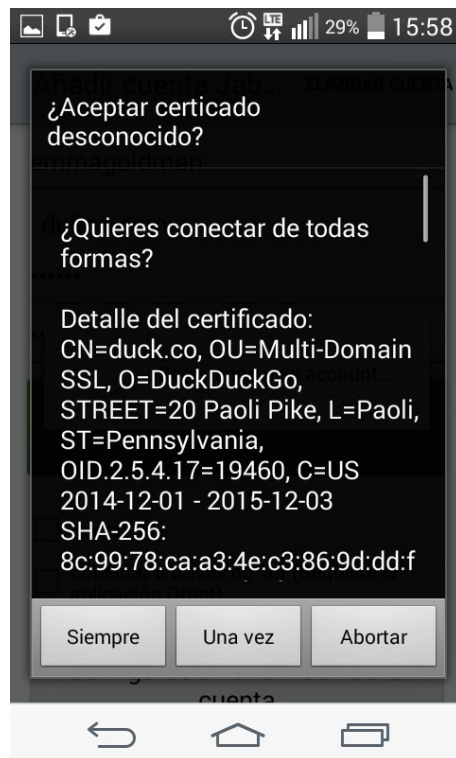
Es importante aclarar que ahora sí estamos ingresando la contraseña de nuestra cuenta en el servidor de dukgo.com. Recomendamos que las contraseñas de la aplicación ChatSecure y de nuestra cuenta en el servidor dukgo.com sean diferentes. También recomendamos desmarcar la opción “**Recordar**”, para que nos solicite la contraseña cada vez que queramos usar nuestra cuenta.

Una vez que ingresamos todos estos datos, y que estamos seguros de recordarlos, registramos nuestra cuenta mediante “**Register Account**”.



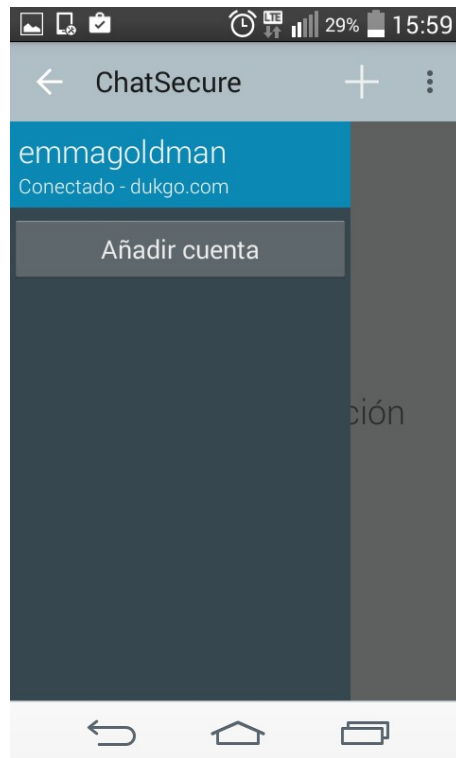
A screenshot of a mobile application interface for registering an account. At the top, there's a status bar with icons for signal, battery (29%), and time (15:58). Below it, a header bar contains the text "Añadir cuenta Jab..." and a link "ELIMINAR CUENTA". The main form has input fields for a username "emmagoldman", a domain "dukgo.com", and two password fields represented by dots. A large green button labeled "Register Account" is positioned below the passwords. Underneath the button are two checkboxes: "Recordar" (unchecked) and "Conectar a través de Tor (Requiere la aplicación Orbot)" (unchecked). At the bottom of the form is a link "Configuración avanzada de la cuenta". The bottom of the screen shows a standard Android navigation bar with back, home, and recent apps icons.

ChatSecure nos preguntará si realmente queremos conectarnos a ese servidor, y le decimos que sí, le damos a “**Siempre**”.



A screenshot of a mobile application interface showing a certificate acceptance dialog. The dialog has a dark background with white text. It starts with the question "¿Aceptar certificado desconocido?". Below this is another question: "¿Quieres conectar de todas formas?". The main body of the dialog contains the following text: "Detalle del certificado: CN=duck.co, OU=Multi-Domain SSL, O=DuckDuckGo, STREET=20 Paoli Pike, L=Paoli, ST=Pennsylvania, OID.2.5.4.17=19460, C=US 2014-12-01 - 2015-12-03 SHA-256: 8c:99:78:ca:a3:4e:c3:86:9d:dd:f". At the bottom of the dialog are three buttons: "Siempre", "Una vez", and "Abortar". The background of the app is visible behind the dialog, showing the same registration form as in the previous screenshot. The bottom of the screen shows the same Android navigation bar.

Luego de eso, nuestra cuenta en dukgo.com ya estará creada y ChatSecure estará conectado a la misma. La opción **“Añadir cuenta”** nos permitiría conectarnos a otra cuenta más, pero como no es lo que nos interesa en este momento, simplemente **no la tocamos**.

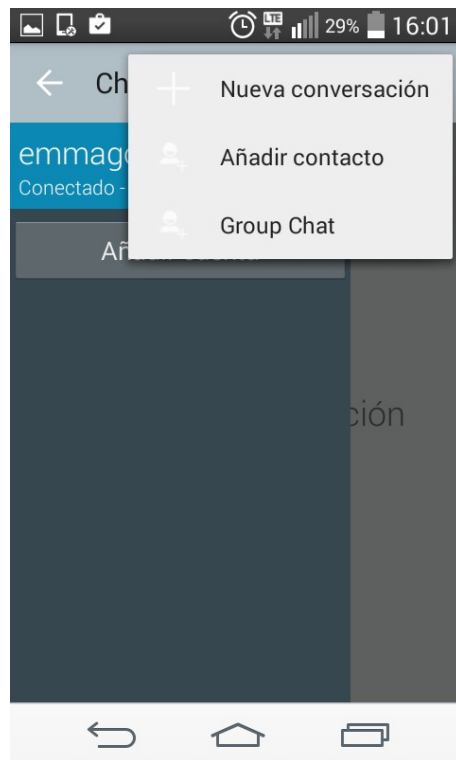


¿Cómo agregamos a una compañera o compañero? para conversar?

En esta sección veremos cómo invitar a otrx compañerx que también hayan creado una cuenta para chatear⁴.

Para agregar a una persona, nos dirigimos al botón que se encuentra en la esquina superior derecha donde nos aparecerán las opciones **“Nueva conversación”**, **“Añadir contacto”** y **“Grupo Chat”**. Elegimos la opción **“Añadir contacto”**.

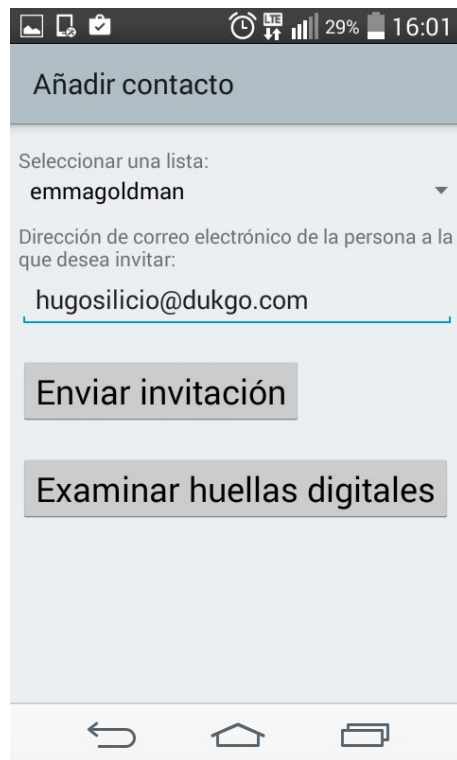
4 Podremos invitar a un/a compañerx siempre y cuando su cuenta de chat funcione mediante el protocolo de mensajería instantánea XMPP, sin importar sobre cuál servidor haya sido dada de alta.



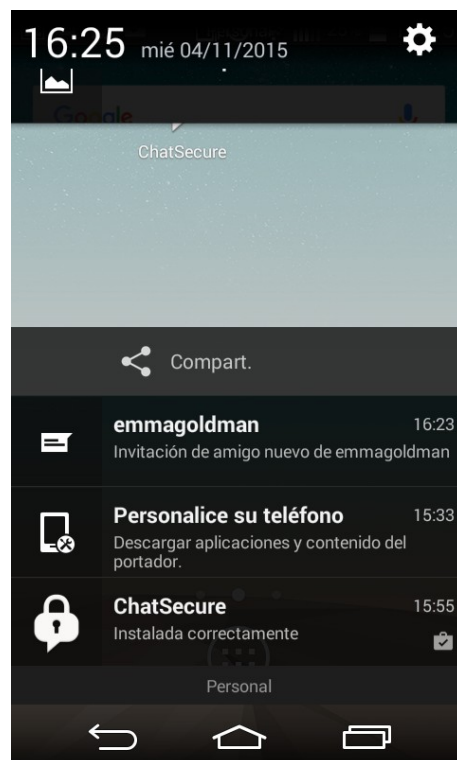
Una vez que elegimos esta opción nos aparecerá un diálogo en el que nos mostrará en **“Seleccionar una lista:”** desde dónde haremos la invitación, en este caso la invitación la haremos desde nuestra cuenta *“emmagoldman”* de *dukgo.com* (no debemos modificar nada en esta opción, simplemente nos muestra desde qué cuenta invitaremos a nuestros compañeros, la opción tiene sentido si tenemos varias cuentas funcionando a la vez en ChatSecure).

En la opción **“Dirección de correo electrónico de la persona a la que desea invitar:”** debemos ingresar la dirección de la cuenta de chat de la persona a la que queremos invitar. Esta dirección se compone de el nombre del usuario o la usuaria, el signo arroba (“@”) y el servidor que utilice nuestros compañeros. En este caso el nombre de usuario al que queremos invitar es *“hugosilicio”* y sabemos que su cuenta está creada en el servidor *“dukgo.com”*, por ende la dirección que ingresaremos es *“hugosilicio@dukgo.com”*.

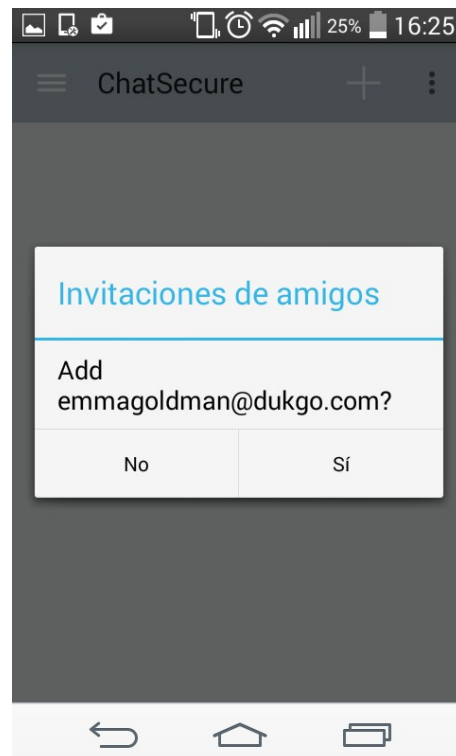
Luego de ingresar estos datos, elegimos **“Enviar invitación”**.



A nuestrox compañerx (*hugosilicio*) la invitación le llegará como una notificación de mensajería, en este caso: “*emmagoldman. Invitación de amigo nuevo de emmagoldman*”



Si nuestrx compañerx accede a la invitación, le pedirá confirmarla. Si accede, nos tendremos mutuamente en nuestras listas de contactos.



Cifrado de las comunicaciones

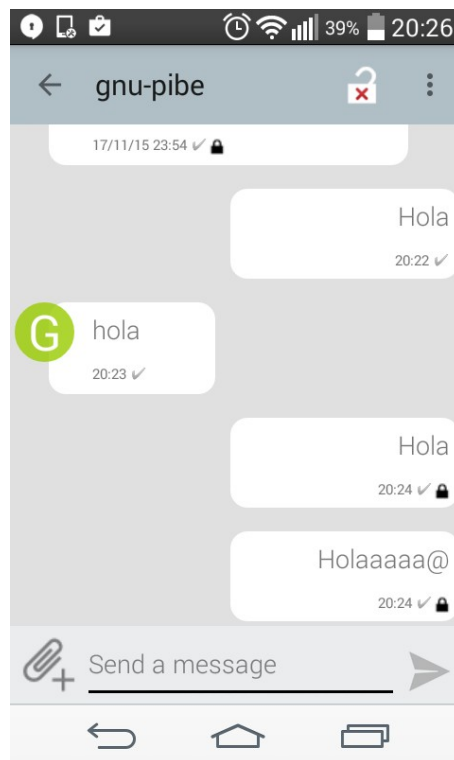
En una pantalla de chat normalmente vemos en la esquina superior izquierda el nombre de la persona con la que estamos conversando (en este caso “*gnu-pibe*”). En la esquina superior-derecha nos mostrará un candado, ese candado nos muestra si nuestra conversación está siendo cifrada o no. Para comunicarnos información sensible (cosas que no queremos que nadie más sepa) con CHATSECURE es necesario que nuestra conversación esté **encriptada**. Encriptar y cifrar quieren decir, en esta instancia, lo mismo.⁵

5 IMPORTANTE: igual recomendamos fuertemente el evitar escribir nombres o términos comprometedores a través de internet desde la computadora o el celular. Nunca hay que abandonar los códigos para hablar discretamente que unx usaría cara a cara.

Si el candado se encuentra **abierto**, entonces la conversación **NO** está siendo encriptada, en cambio cuando el candado se muestre **cerrado** el cifrado de la comunicación **SÍ** está en funcionamiento, protegiendo los mensajes intercambiados de la interceptación en tránsito por parte de intrusxs.

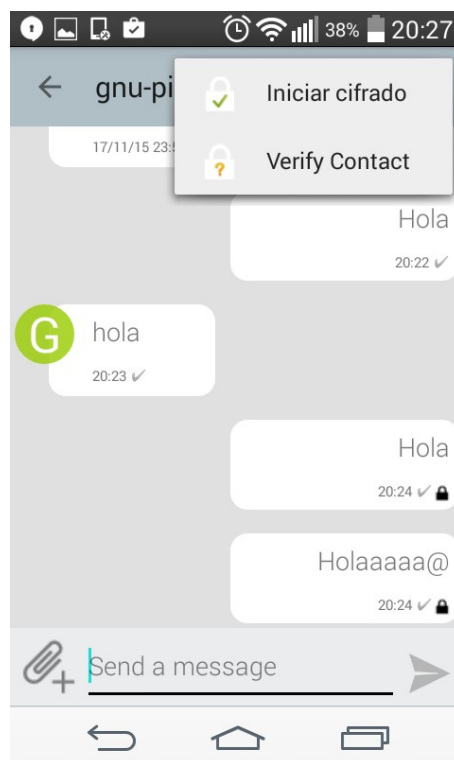
A demás, ChatSecure nos muestra mensajes confirmando y avisando del estado actual de la conversación.

En esta sección veremos cómo activar el cifrado en una conversación.



Activar el cifrado

Es importante mirar siempre que el cifrado esté activo, es decir, que el candado esté cerrado. Si el candado está abierto pulsamos sobre él y elegimos “**Iniciar cifrado**”. El candado pasará a estar cerrado con un signo de interrogación amarillo en su interior.

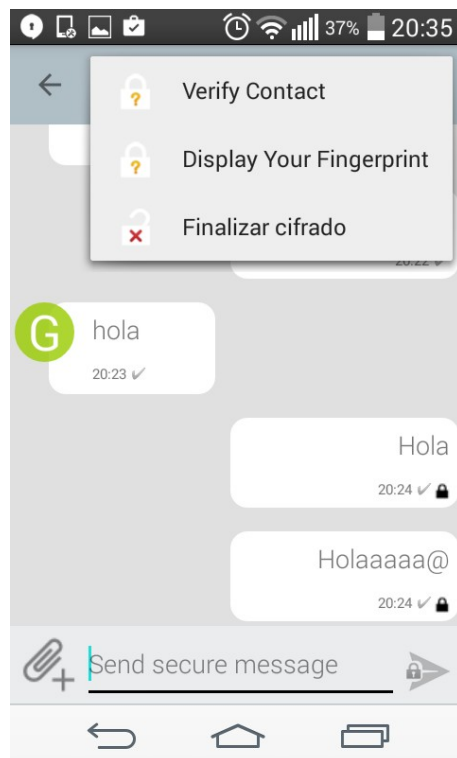


Una cuestión de gran importancia en la seguridad de nuestra comunicación, es asegurarnos de que quien está del otro lado sea quien dice ser, es decir la **autenticación**. En nuestra cotidianeidad hacemos esta verificación constantemente, al vernos las caras o reconociéndonos la voz, sin embargo en medios digitales la suplantación de identidad es muy común porque no hay medios tan inmediatos de autenticación.

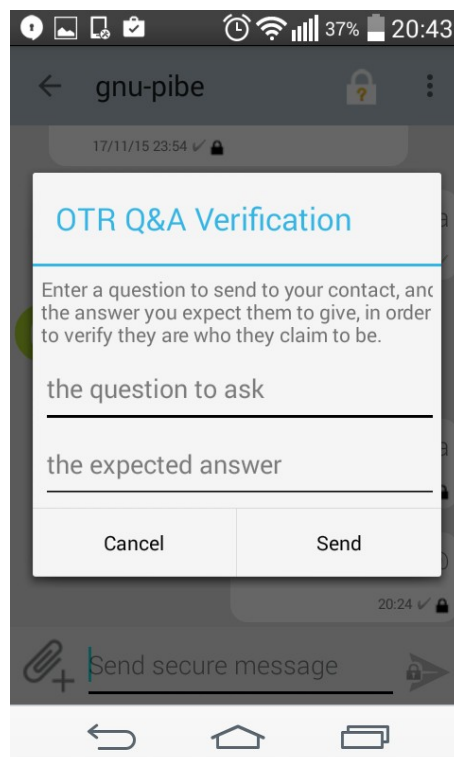
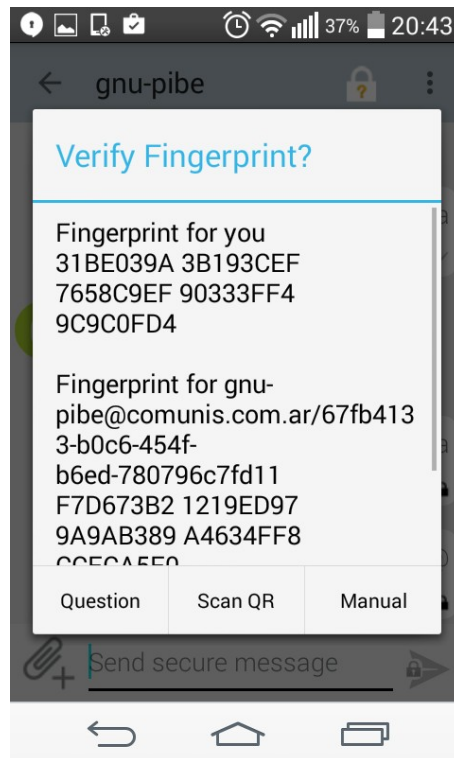
Un mecanismo que nos ofrece ChatSecure para este fin es pregunta y respuesta, que consiste en preguntar por algo que sólo la persona con quien queremos comunicarnos podría conocer.

Cómo autenticar

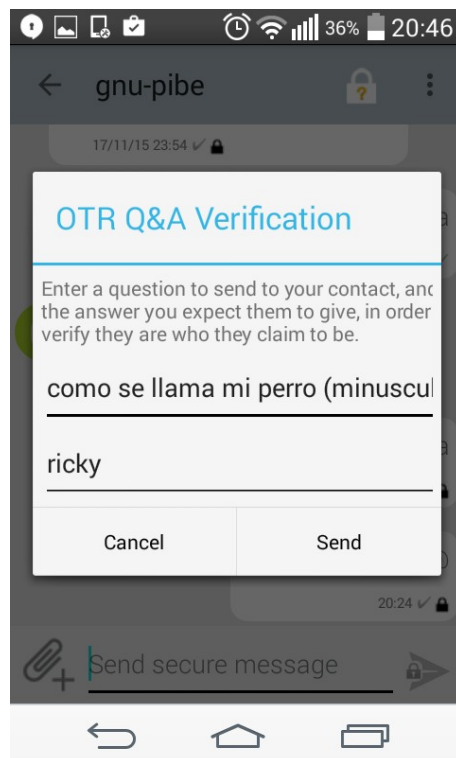
Cuando ChatSecure nos muestra el logo del candado con un signo de interrogación es necesario autenticar. Para ello apretamos en el logo del candado y elegimos “**verify contact**”.



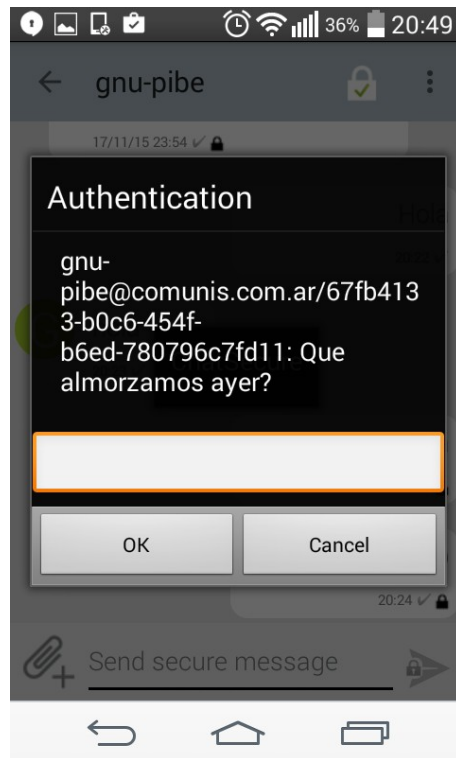
Luego elegimos el método de "pregunta y respuesta", que nos aparecerá como "Question".



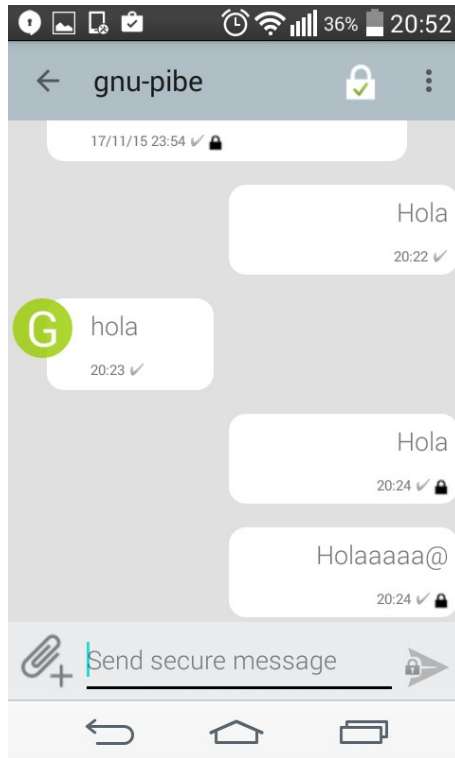
La pregunta que hagamos tiene que ser muy clara y concreta con sólo una respuesta posible, la respuesta debe ser una sola palabra. Debería ser algo muy específico que sólo las personas que se comunican sepan, sino cualquiera podría responder. Supongamos que mi perro se llama Ricky, así que le voy a preguntar a la otra persona cómo se llama mi perro (suponiendo que lo sabe). Le envío la pregunta “**como se llama mi perro (minúscula)**”, aclaro que la respuesta debe estar en minúscula porque deseo que me responda “**ricky**”. Si me responden “Ricky”, con mayúscula, dará error.



Ahora mi compañerx debe autenticarme a mí. En este caso, me envió la pregunta “**Que almorzamos ayer?**”, yo se que la respuesta es “**milanesa**”, así que la ingreso.



Si la coloqué bien, el candadito debe verse con una tilde verde en su interior.



Ahora cada vez que nuestrx compañerx nos contacte desde el mismo equipo y la misma cuenta, CHATSECURE lo reconocerá y por tanto no es necesario autenticar. Acá cobra importancia la primera contraseña que configuramos al comenzar con CHATSECURE, porque nos garantiza que quien sabe esa contraseña es quien está autenticado, y no otra persona, por ejemplo alguien que haya sustraído el celular a nuestrx compañerx.

Ahora estamos en condiciones de tener con nuestrx compañerx una conversación segura, en el servidor de DuckDuckGo, mediante el protocolo XMPP y cifrada con OTR.

Terminar una conversación

Es importante que cuando terminamos de conversar con nuestrox compañerx le indiquemos esto a CHATSECURE, para que elimine dicha conversación y olvide la clave de cifrado especial para esa conversación.

Esto lo hacemos pulsando sobre el candado que se muestra en la parte superior derecha y eligiendo la opción “**end chat**”.

A MODO DE CIERRE

Dedicamos este material a compartir y construir conocimientos sobre herramientas que pueden aportar a hacer más confiables nuestras comunicaciones digitales. Ahora hacemos un llamado para que se difunda y, sobre todo, para poner a prueba lo dicho.

Comprendemos que la seguridad en las comunicaciones de una organización social dependerá en gran medida de la vocación que tengamos para construirla y sostenerla en el tiempo. Remarcamos nuevamente que se trata de un proceso colectivo, en que todxs debemos asumir conscientemente la responsabilidad de proteger a nuestroxs compañerxs y a la organización. Invitamos a seguir problematizando cómo nos comunicamos, así iremos construyendo alternativas cada vez más firmes. "No se trata de temer o esperar, sino de buscar nuevas armas"⁶

6 Gilles Deleuze, Posdata sobre las sociedades de control.

GLOSARIO

Código abierto: el acceso libre al código de programación en el que está escrito un programa, para que cualquier persona con los conocimientos adecuados pueda estudiarlo, mejorarlo y compartirlo con la comunidad.

Encriptación: método para cifrar las comunicaciones en clave, mediante sustituciones logradas gracias al procesamiento informático de algoritmos matemáticos complejos.

Metadatos: información que acompaña (por ej.) al contenido propio de una comunicación, como pueden ser la identidad de los participantes, hora de los mensajes, ubicación física y dispositivos utilizados.

Navegador: programa para visualizar páginas web a través de una conexión a internet.

OTR: siglas de “Off-The-Record” (“confidencialmente”), sistema de cifrado en clave para mensajes de chat.

Servidores: computadoras de gran capacidad que funcionan permanentemente para ofrecer servicios en línea, alojando información y otorgando acceso a ella.

Sistema operativo: “programa” o interfaz general que permite la ejecución de programas o aplicaciones para tareas específicas. Los ejemplos más difundidos son el Windows de Microsoft y Android de Google (ambos comerciales y privativos).

XMPP: lenguaje técnico en común que reconocen distintos servidores de chat compatibles entre sí, como los de dukgo.com y riseup.net.